20ET20*0624nn860

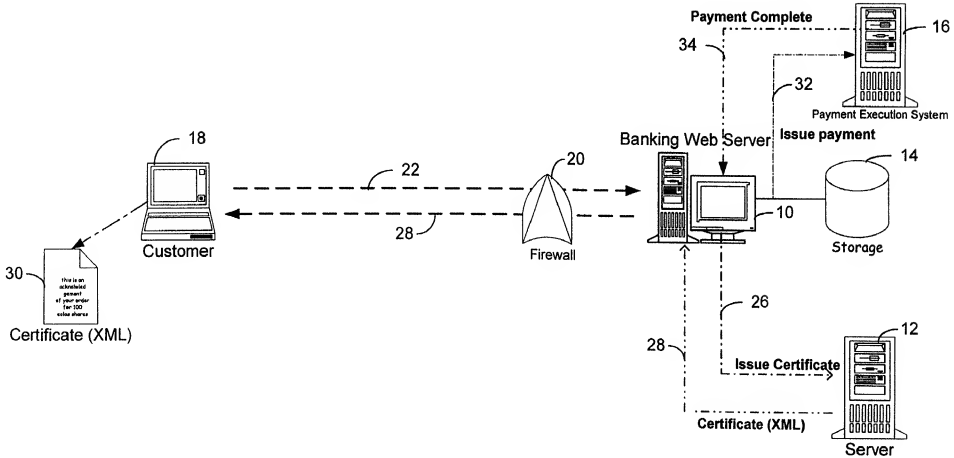


FIG. 1

20CT20 05:44:860

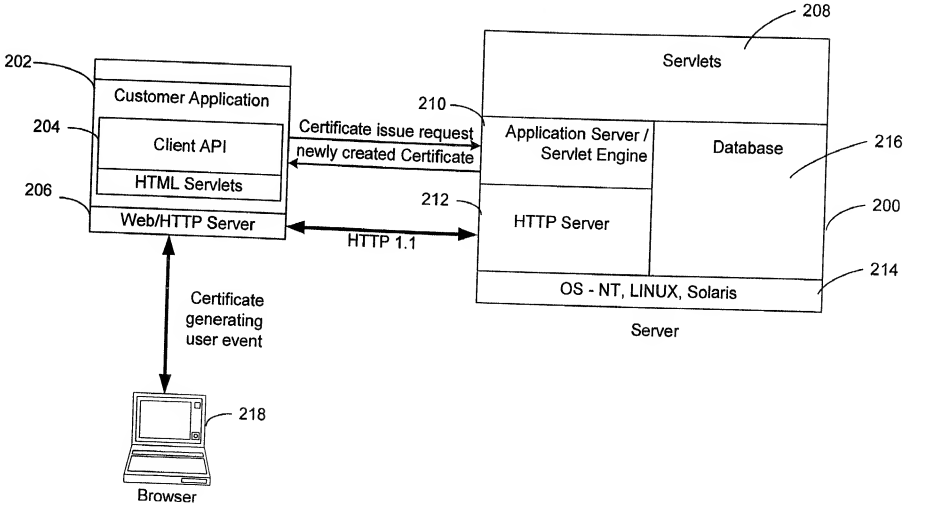
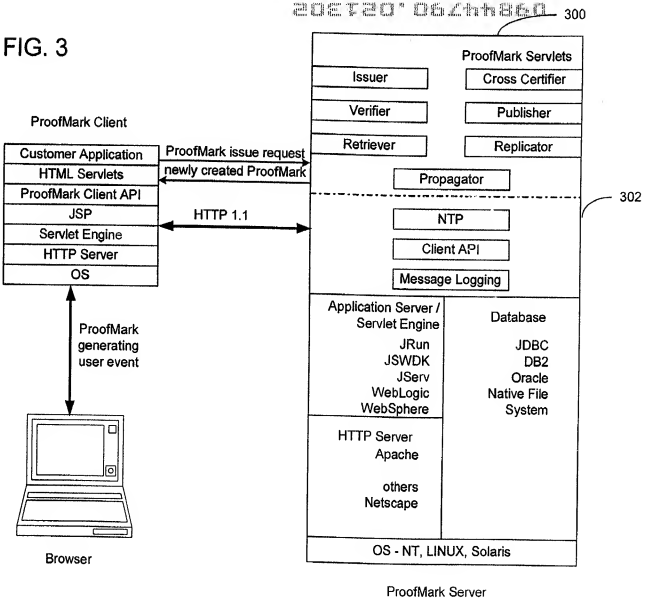


FIG. 2

FIG. 3


300
ProofMark Servlets
Issuer
Cross Certifier
Verifier
Publisher
Retriever
Replicator
Propagator
302
NTP
Client API
Message Logging
ProofMark Client
Customer Application
HTML Servlets
ProofMark Client API
JSP
Servlet Engine
HTTP Server
OS
ProofMark issue request
newly created ProofMark
HTTP 1.1
ProofMark generating user event
Application Server / Servlet Engine
JRun
JSWDK
JServ
WebLogic
WebSphere
Database
JDBC
DB2
Oracle
Native File System
HTTP Server
Apache
others
Netscape
OS - NT, LINUX, Solaris
Browser
ProofMark Server

20070720.0647.3801

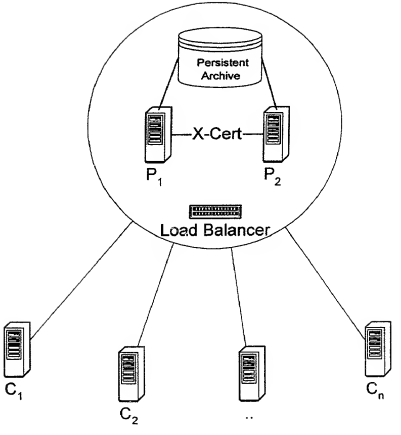


FIG. 4

20070120.0744850

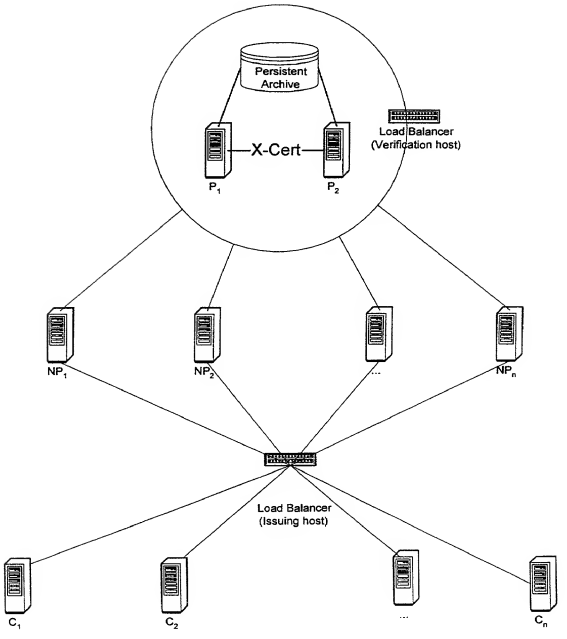


FIG. 5

20070720.0624390

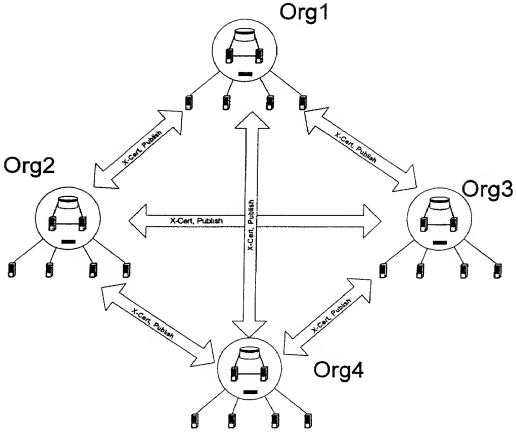


FIG. 6

20ET20'06Zhh860

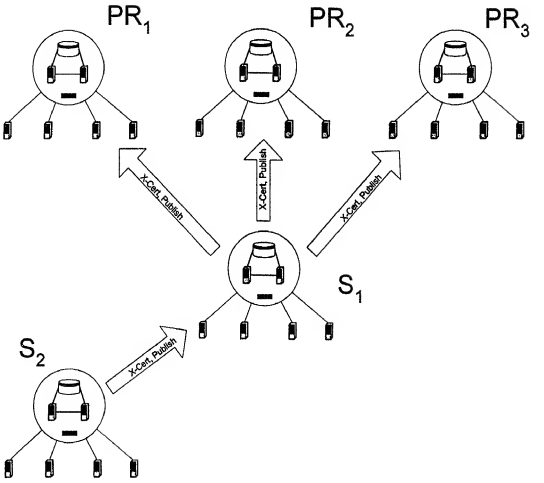


FIG. 7

20120706.4860

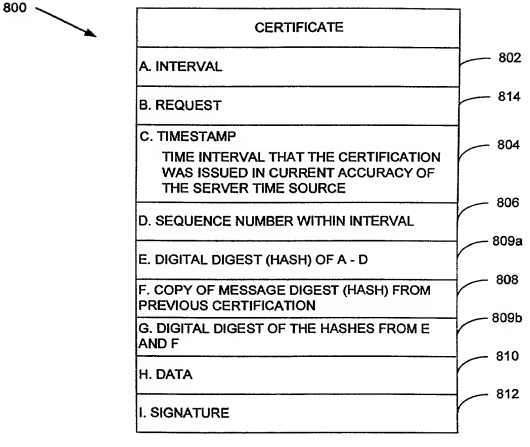


FIG. 8

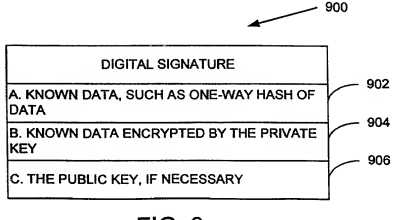


FIG. 9

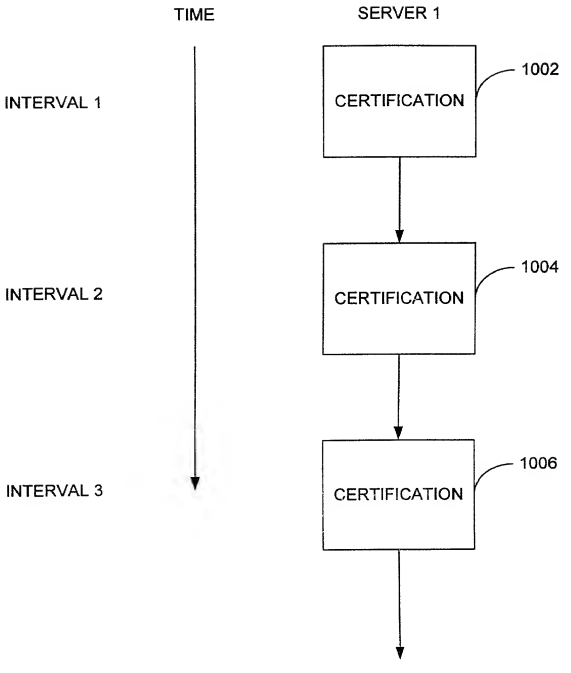

TIME
SERVER 1
INTERVAL 1
INTERVAL 2
INTERVAL 3
CERTIFICATION
CERTIFICATION
CERTIFICATION
1002
1004
1006

FIG. 10

20CT20.05244860

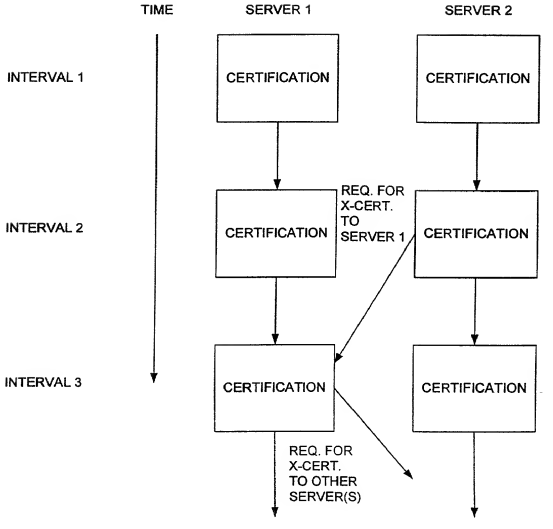


FIG. 11

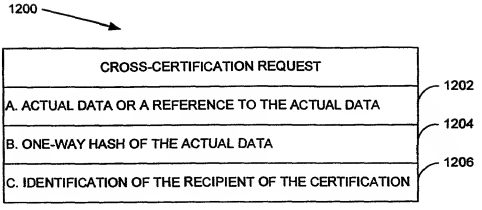


FIG. 12

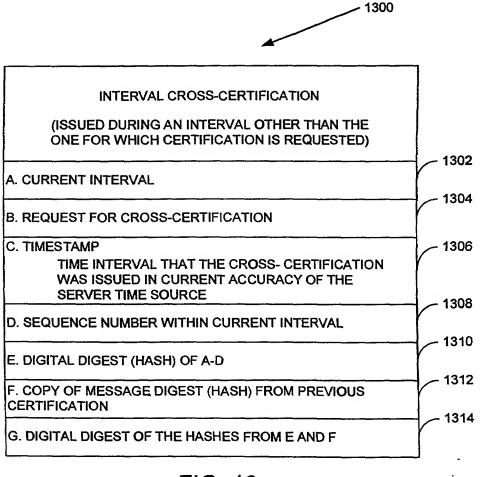


FIG. 13

05844790.021202

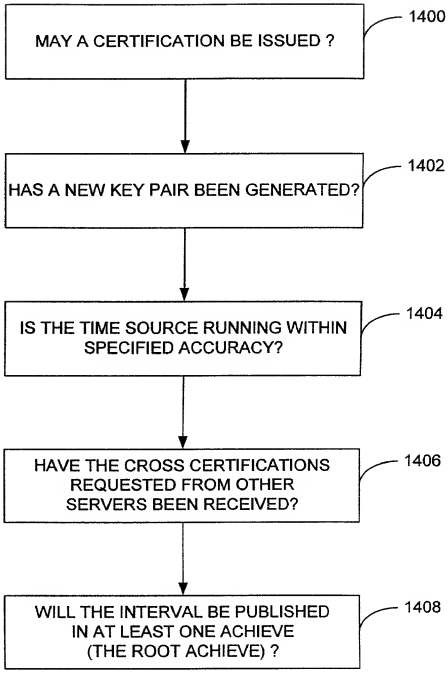


FIG. 14

20120*0674886

2014-06-20 06:41:06

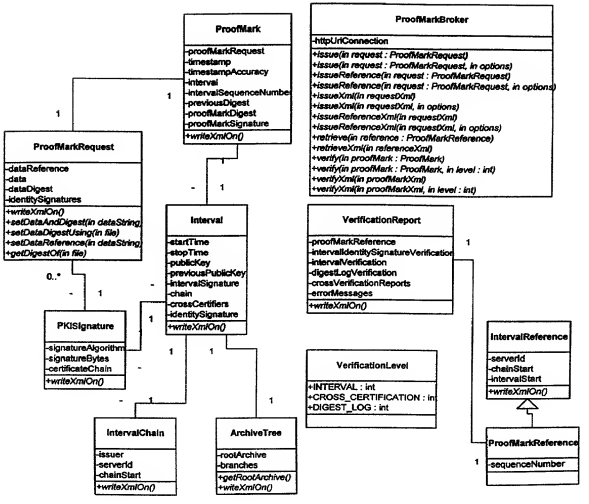


FIG. 15

20120706.1826

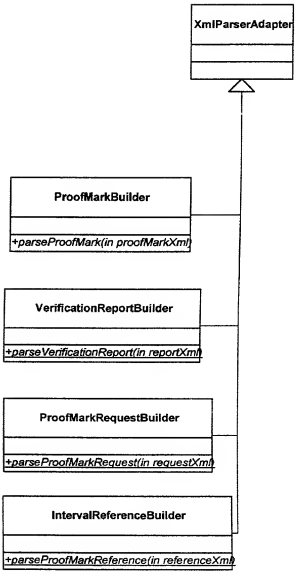


FIG. 16

2017-10-06 14:36:50

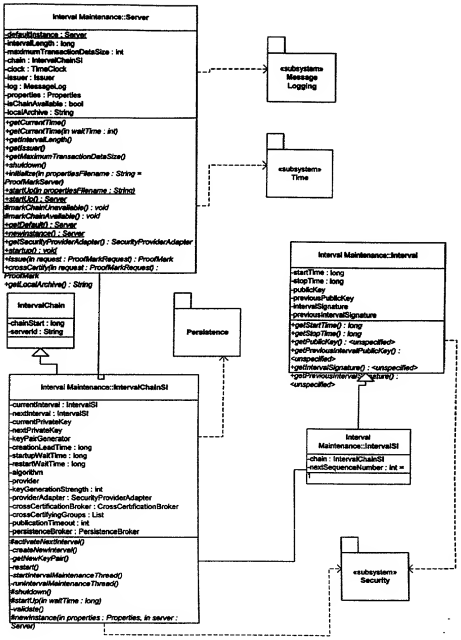


FIG. 17

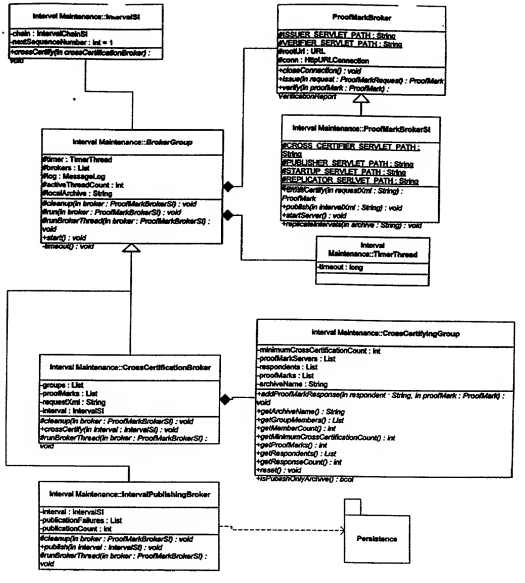

Interval Maintenance::IntervalSI
-chain : IntervalChainSI
-nextSequenceNumber : Int = 1
+crossCertify(in crossCertificationBroker) : void
ProofMarkBroker
#ISSUER_SERVLET_PATH : String
#VERIFIER_SERVLET_PATH : String
#hostUrl : URL
#conn : HttpURLConnection
+closeConnection() : void
+issue(in request : ProofMarkRequest) : ProofMark
+verify(in proofMark : ProofMark) : VerificationReport
Interval Maintenance::ProofMarkBrokerSI
#CROSS_CERTIFIER_SERVLET_PATH : String
#PUBLISHER_SERVLET_PATH : String
#STARTUP_SERVLET_PATH : String
#REPLICATOR_SERVLET_PATH : String
+crossCertify(in requestUrl : String) : ProofMark
+publish(in intervalUrl : String) : void
+startServer() : void
+replicateIntervals(in archive : String) : void
Interval Maintenance::BrokerGroup
#timer : TimerThread
#brokers : List
#log : MessageLog
#activeThreadCount : Int
#localArchive : String
#cleanup(in broker : ProofMarkBrokerSI) : void
#run(in broker : ProofMarkBrokerSI) : void
#runBrokerThread(in broker : ProofMarkBrokerSI) : void
+start() : void
-timeout() : void
Interval Maintenance::TimerThread
-timeout : long
Interval Maintenance::CrossCertifyingGroup
-minimumCrossCertificationCount : Int
-proofMarkServers : List
-respondents : List
-proofMarks : List
-archiveName : String
+addProofMarkResponse(in respondent : String, in proofMark : ProofMark) : void
+getArchiveName() : String
+getGroupMembers() : List
+getMemberCount() : int
+getMinimumCrossCertificationCount() : int
+getProofMarks() : int
+getRespondents() : List
+getResponseCount() : int
+reset() : void
+isPublishOnly/Archive() : bool
Interval Maintenance::CrossCertificationBroker
-groups : List
-proofMarks : List
-requestXml : String
-interval : IntervalSI
#cleanup(in broker : ProofMarkBrokerSI) : void
+crossCertify(in interval : IntervalSI) : void
#runBrokerThread(in broker : ProofMarkBrokerSI) : void
Interval Maintenance::IntervalPublishingBroker
-interval : IntervalSI
-publicationFailures : List
-publicationCount : Int
#cleanup(in broker : ProofMarkBrokerSI) : void
+publish(in interval : IntervalSI) : void
#runBrokerThread(in broker : ProofMarkBrokerSI) : void
Persistence

FIG. 18

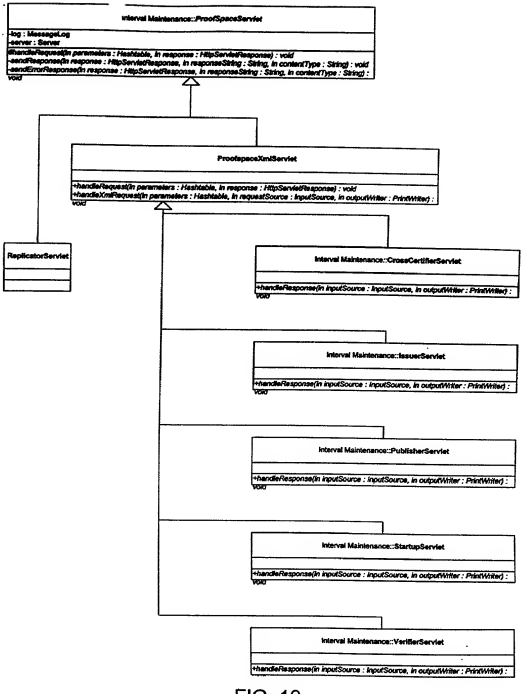


FIG. 19

20030120.0644960

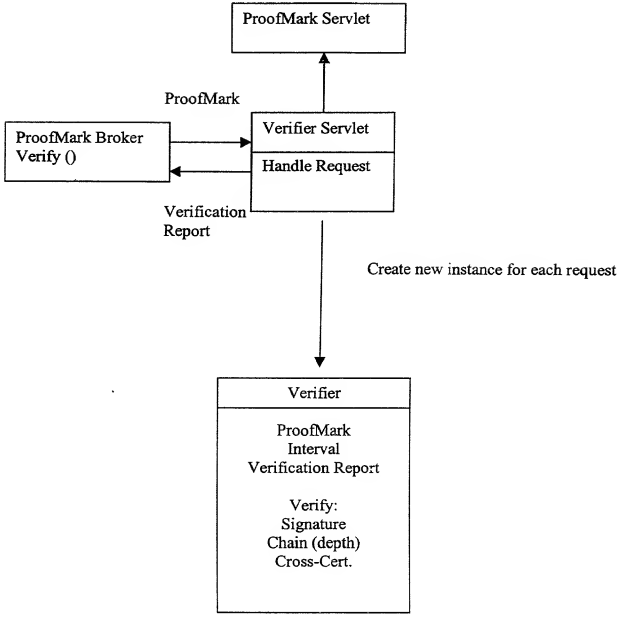

ProofMark Servlet
ProofMark
ProofMark Broker
Verify ()
Verifier Servlet
Handle Request
Verification
Report
Create new instance for each request
Verifier
ProofMark
Interval
Verification Report
Verify:
Signature
Chain (depth)
Cross-Cert.

FIG. 20

20120706744860

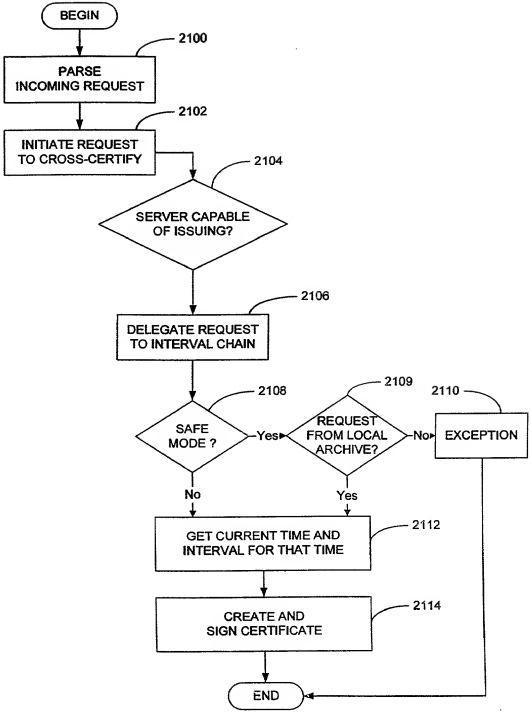


FIG. 21

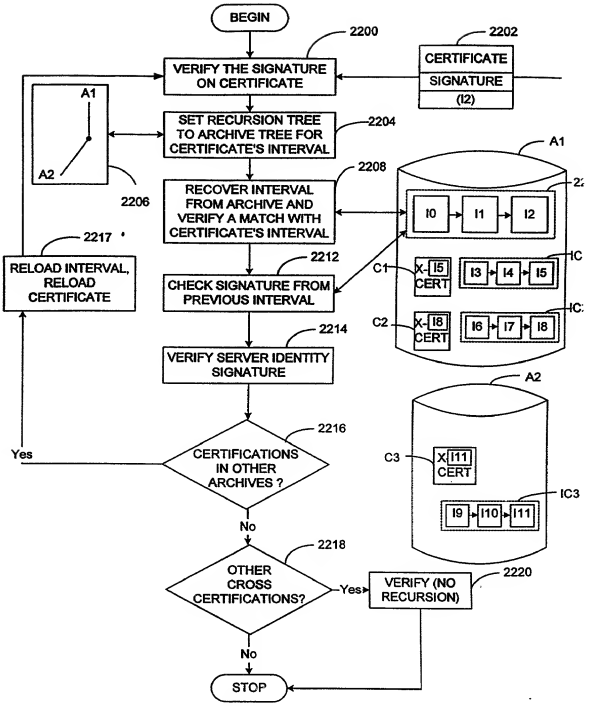

BEGIN
2200
VERIFY THE SIGNATURE ON CERTIFICATE
2202
CERTIFICATE
SIGNATURE
(I2)
A1
A2
2206
SET RECURSION TREE TO ARCHIVE TREE FOR CERTIFICATE'S INTERVAL
2204
RECOVER INTERVAL FROM ARCHIVE AND VERIFY A MATCH WITH CERTIFICATE'S INTERVAL
2208
2217
RELOAD INTERVAL, RELOAD CERTIFICATE
2212
CHECK SIGNATURE FROM PREVIOUS INTERVAL
2214
VERIFY SERVER IDENTITY SIGNATURE
2216
CERTIFICATIONS IN OTHER ARCHIVES ?
Yes
No
2218
OTHER CROSS CERTIFICATIONS?
Yes
2220
VERIFY (NO RECURSION)
No
STOP
A1
I0
I1
I2
C1
X I5 CERT
I3
I4
I5
C2
X I8 CERT
I6
I7
I8
A2
C3
X I11 CERT
IC3
I9
I10
I11

FIG. 22

xxxx yyyy zzzz
xxxx yyyy zzzz
aaa bbb
aaa bbb
ccc ddd
ccc ddd
eee ffffff gggg
eee ffffff gggg
hhh
hhh
iiiiiiiii
iiiiiiiii
kkk
kkk

FIG. 23

20C120 06/44860

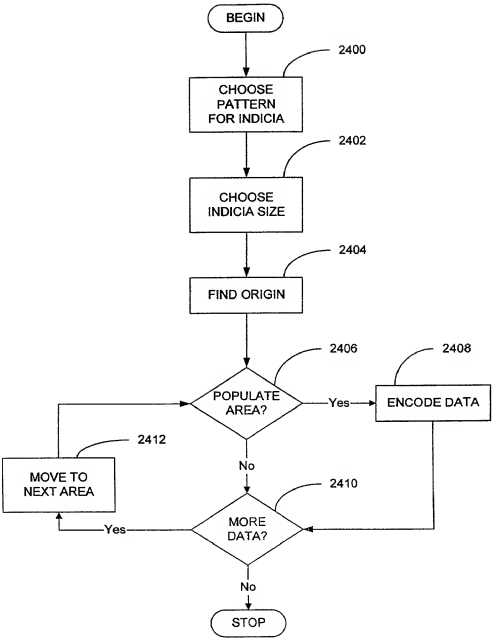


FIG. 24

20C120 "06744860

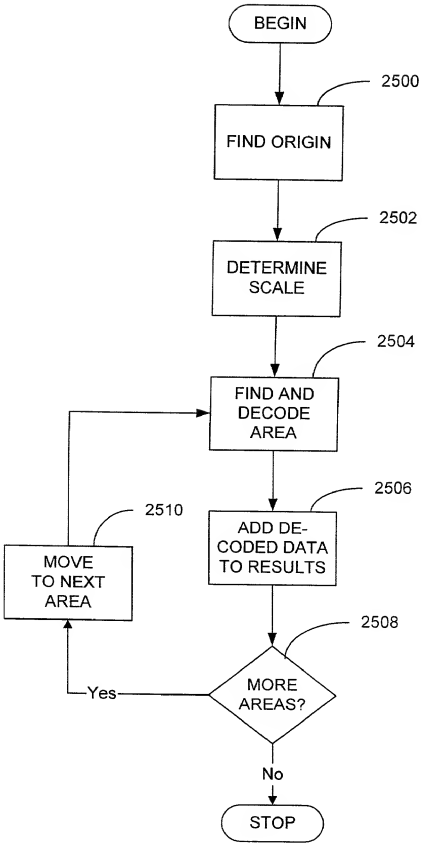


FIG. 25

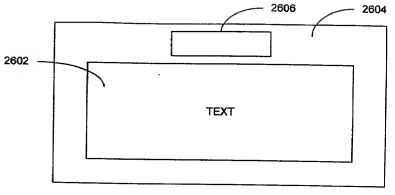


FIG. 26

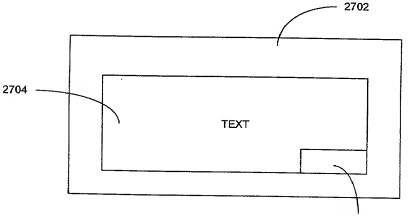


FIG. 27

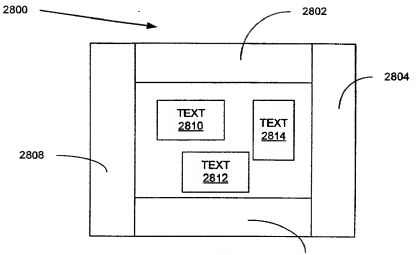


FIG. 28

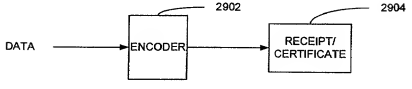


FIG. 29

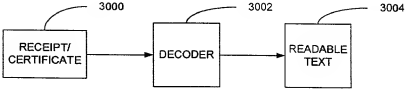


FIG. 30

20070306744860